WHAT IS CLAIMED IS:

1. An information reproducing apparatus, comprising:

a secure module that stores a first information, wherein the secure module can not be accessed from outside;

a memory that stores a second information, wherein the memory can be accessed from outside; and

a falsification checking unit that is loaded on the secure module, wherein the falsification checking unit reads the second information from the memory by direct access, compares the second information with the first information in the secure module, and checks a falsification of the second information based on a result of the comparison.

2. The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads all of the second information.

3. The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads a part of the second information.

4. The information reproducing apparatus according to claim 1, wherein the falsification checking unit performs the comparison of the first information and the second information using a checksum method.

5. The information reproducing apparatus according to claim 1, wherein the second information is software.

6. The information reproducing apparatus according to claim 1, wherein the falsification checking unit reads the second information from the memory on an irregularly basis.

7. The information reproducing apparatus according to claim 1, further comprising:

an updating unit that is loaded on the secure module and that updates the second information in the memory using a direct access method, wherein

the falsification checking unit reads the second information updated by the updating unit.

8. The information reproducing apparatus according to claim 7, wherein the updating unit updates the second information on an irregularly basis.

9. The information reproducing apparatus according to claim 7, wherein the updating unit updates a part of the second information.

10. The information reproducing apparatus according to claim 1, further comprising:

a storage control unit that is loaded on the secure module,

wherein the storage control unit changes original information, and stores the changed information as the second information into the memory.

11. The information reproducing apparatus according to claim 10, wherein when the second information is updated, the storage control unit hands over the second information from the pre-updating information to the post-updating information.

12. The information reproducing apparatus according to claim 10, wherein the storage control unit encrypts the original information using a key that exists in the secure module, and stores the encrypted original information as the second information into the memory.

13. The information reproducing apparatus according to claim 1, further comprising:

a key managing unit that is loaded on the secure module, wherein the key managing unit holds a key used to encrypt or decode the second information, and the key managing unit supplies the key to the storage control unit, if the falsification checking unit does not detect a falsification.

14. The information reproducing apparatus according to claim 13, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

15. The information reproducing apparatus according to claim 13, wherein the key managing unit changes the key each time the key managing unit supplies the key to the storage control unit.

16. The information reproducing apparatus according to claim 13, wherein when the falsification checking unit detects a falsification, the key managing unit does not supply the key to the storage control unit.

17. The information reproducing apparatus according to claim 1, further comprising:

a writing unit that is loaded on the secure module, wherein the writing unit writes a secret information within the secure module into the memory as the second information using the direct access method, wherein

the falsification checking unit checks falsification of the second information based on response information corresponding to the secret information.

18. The information reproducing apparatus according to claim 17, wherein the secret information is stored in a controlled memory space, wherein

the controlled memory space is such that a normal information is read out from the memory space at a first time and a different information is read out at a second time.

19. The information reproducing apparatus according to claim 1, wherein the second information is encrypted MPEG data.

20. An information reproducing method comprising:

a reading step, which is executed within a secure module, of reading second information stored in a memory, wherein the secure module stores a first information, and the secure module can not be accessed from outside, and the memory can be accessed from outside using a direct access method; and

a falsification checking step of comparing the second information with the first information, and checking a falsification of the second information based on a result of the comparison.

21. A secure module mounted to an information reproducing apparatus, comprising:

a reading unit that reads a second information from a memory mounted to a information reproducing apparatus by direct access, the memory can be accessed from outside; and;

a falsification checking unit that compares the second information with a first information in the secure module, and checks a falsification of the second information based on a result of the comparison.

22. The secure module according to claim 21, wherein the reading unit reads all of the second information.

23. The secure module according to claim 21, wherein the reading unit reads a part of the second information.

24. The secure module according to claim 21, wherein the falsification checking unit performs the comparison of the first information and the second information using a checksum method.

25. The secure module according to claim 21, wherein the second information is software.

26. The secure module according to claim 21, wherein the reading unit reads the second information from the memory on an irregularly basis.

27. The secure module according to claim 21, further comprising:

an updating unit that updates the second information in the memory using a direct access method, wherein

the falsification checking unit reads the second information updated by the updating unit.

28. The secure module according to claim 27, wherein the updating unit updates the second information on an irregularly basis.

29. The secure module according to claim 27, wherein the updating unit updates a part of the second information.

30. The secure module according to claim 21, further comprising:

a storage control unit that changes original information, and stores the changed information as the second information into the memory.

31. The secure module according to claim 30, wherein when the second information is updated, the storage control unit hands over the second information from the pre-updating information to the post-updating information.

32. The secure module according to claim 30, wherein the storage control unit encrypts the original information using a key that exists in the secure module, and stores the encrypted original information as the second information into the memory.

33. The secure module according to claim 21, further comprising:

a key managing unit that holds a key used to encrypt or decode the second information, and the key managing unit supplies the key to the storage control unit, if the falsification checking unit does not detect

a falsification.

34. The secure module according to claim 33, wherein the key supplied by the key managing unit is valid only for a predefined period of time.

35. The secure module according to claim 33, wherein the key managing unit changes the key each time the key managing unit supplies the key to the storage control unit.

36. The secure module according to claim 33, wherein when the falsification checking unit detects a falsification, the key managing unit does not supply the key to the storage control unit.

37. The secure module according to claim 21, further comprising:

a writing unit that writes a secret information within the secure module into the memory as the second information using the direct access method, wherein

the falsification checking unit checks falsification of the second information based on response information corresponding to the secret information.

38. The secure module according to claim 37, wherein the secret information is stored in a controlled memory space, wherein

the controlled memory space is such that a normal information is

read out from the memory space at a first time and a different information is read out at a second time.

39. The secure module according to claim 21, wherein the second information is encrypted MPEG data.

40. A recording medium that records a program for causing a secure module mounted to an information reproducing apparatus to execute a process, the program causes the secure module to execute steps of:

a reading step of reading a second information stored in a memory mounted to the information reproducing apparatus, wherein the secure module stores a first information, and the secure module can not be accessed from outside, and the memory can be accessed from outside using a direct access method; and

a falsification checking step of comparing the second information with the first information, and checking a falsification of the second information based on a result of the comparison.